**TP Chiffrement**

On considère deux interlocuteurs **A** et **B**.

Chacun possède un couple clef publique/ clef privée : (KA, KA’) et (KB, KB’) respectivement.

**A** envoie un message **m** à **B**

1. De quel chiffrement s’agit-il ?

Chiffrement asymétrique

1. Expliquez le message **mc** chiffré. Avec quel algorithme de chiffrement a-t-on chiffrer ce message ?

mc = m +KB + Algo de chiffrement

1. **B** déchiffre le message de **A** et le nomme **md**. Expliquez ce message déchiffré

md = mc +KB’+ Algo de déchiffrement

1. **B** répond à **A** avec un message **m’**. Expliquez ce message. Avec quel algorithme peut-on chiffrer ce message ?

m’ = KA + md + Algo de chiffrement

1. De quel chiffrement s’agit-il ?

Chiffrement asymétrique

1. Quels sont les avantages de ce type de chiffrement ? Quels en sont les inconvénients ?

|  |  |
| --- | --- |
| AVANTAGES | INCONVENIENTS |
| Robustesse des algo Plus sécurisé | Lenteur |
| Longueur des bits donc plus sécurisé |  |
|  |  |

1. Avec quel autre algorithme de chiffrement pouvait-il chiffrer ce message ?

RSA, El Gamal, DSA, Diffie Hellman

1. **A** souhaiterais à nouveau envoyer un message à **B** et ne dispose plus des clés de **B**. Avec quelle clé peut-il envoyer un message à **B** ? Où peut-il la trouver par exemple ?

KA, Serveur des Clés

1. **A** génère une clé de session et souhaiterais l’envoyer à **B.** Comment procèdera-t-il ?

Chiffrer Kc avec KB et envoyer ; Algo Diffie Hellman

1. On apprend qu’un utilisateur **C** avait dérobé la clé privée de **B** avant cet échange quelle(s) caractéristique(s) de sécurité sont alors compromise(s) ?

Confidentialité, Intégrité, non-répudiation, Authenticité